USAWC STRATEGY RESEARCH PROJECT

INFORMATION TECHNOLOGY CHALLENGES FACING THE STRATEGIC LEADERS OF HOMELAND SECURITY IN THE 21ST CENTURY.

by

Mr. Dan Alexander
Department of the Navy

Colonel Larry Godfrey
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
03 MAY 2004		**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Technology Challenges Facing the Strategic Leaders of Homeland Security in the 21st Century	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Dan Alexander	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**23**	

ABSTRACT

AUTHOR: Dan Alexander

TITLE: INFORMATION TECHNOLOGY CHALLENGES FACING THE STRATEGIC LEADERS OF HOMELAND SECURITY IN THE 21ST CENTURY.

FORMAT: Strategy Research Project

DATE: 19 March 2004 PAGES: 23 CLASSIFICATION: Unclassified

This paper examines the Information Technology challenges that face strategic leaders of the Department of Homeland Security (DHS) as the United States transitions into the 21st Century. Author assumes that Information Technology is the enabler to providing the Department of Homeland Security a high fidelity, effective, and operational infrastructure and is critical to the overall success of the Global War on Terrorism. The author reviews and discusses options for maintaining an effective infrastructure of Information Technology that protects the vital interests of the U.S. homeland. Author argues that by having positive control of the five (5) challenging areas of cultural change, systems integration, knowledge management, decision-making, and telecommunications, DHS can successfully maintain an efficient and effective organization that will provide a protective wall between terrorist activities and the homeland of the United States.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I would like to take this opportunity to acknowledge several people who assisted me in the completion of this paper. First, I want to thank Colonel Larry Godfrey, my project advisor at the Army War College. He gave me invaluable assistance in focusing my efforts, then reviewed and provided editorial comments of multiple drafts of this paper, and constantly motivated me to complete this paper to the best of my ability.

I would also like to acknowledge my classmates and seminar "5" partners who provided an extraordinary support structure of encouragement that continues to this day. A special thanks to all of these folks (Glenn Starnes, Lee Gutierrez, Bill Rapp, Joel Hillison, Carlos Gomez, Steve Fraunfelter, Janie Hopkins, Dave Bishop, John Moore, George Fella, Chuck Johnson, Stan Butlak, TC McMullen, David Glover, Virgil Williams, Tom Riddle, Mark Montesclaros, Diane DiClemente, Joe Nunez, John Bonin, and Steve Nerheim).

INFORMATION TECHNOLOGY CHALLENGES FACING THE STRATEGIC LEADERS OF HOMELAND SECURITY IN THE 21ST CENTURY

In war while everything is simple, even the simplest thing is difficult.

—Clausewitz

In July 2002, the Office of Homeland Security issued the National Strategy for Homeland Security. The purpose was to mobilize and organize the nation to secure the United States from terrorists attacks. It also identified six mission areas of protection (intelligence and warning, border and transportation security, domestic counter terrorism, protecting critical infrastructure, defending against catastrophic threats, and emergency preparedness and response). [1] National Strategy for Homeland Security has made it clear that more money spent does not equate to more security earned because terrorist activities continue to this day. Information Technology (IT) will be the enabler that the Department of Homeland Security (DHS) intends to use to meet full functionality in the six mission areas of protection. This paper provides various guidelines and ideas to assist the strategic leaders in the DHS to provide a future information technology infrastructure that supports programs for homeland safety and security.

The strategic leaders of DHS face a daunting task for the next 10-20 years. There is no method for prioritizing the challenges that will provide a roadmap for success in the immediate future. This paper can only give an overview of guidance for the strategic leader and provide assistance with various recommendations. Offering any type of roadmap for DHS strategic leaders could result in misdirection that might hamper progress. For example, a roadmap could provide for specific focal areas that don't necessarily improve overall security within the homeland. Strategic leaders must maintain an open mind receptive to new ideas and new conceptual directions. I believe that the atmosphere for strategic leaders within DHS will be volatile and uncertain for at least the next 20 years or longer, depending on future terrorist levels.

DHS strategic leaders must continually look into the future for Information Technology capabilities being developed. For instance, if General Lee had had email capability during the battle of Gettysburg, the results might have been significantly different. The leadership at DHS will have to gain, and maintain, a competitive advantage over any future homeland security threats. In order for strategic leaders at DHS to maintain the competitive edge over time, specific IT challenges must be identified, addressed and solved. The IT linked challenges are cultural change, systems integration, knowledge management, decision-making, and telecommunications. It is my argument that by having positive control of these 5 challenging areas, DHS can successfully maintain an efficient and effective organization that will provide a

protective wall between terrorist activities and the homeland of the United States. Cultural change will be a constant resistive force facing the current DHS leadership. Combining 22 organizations which have different cultures into the Department of Homeland Security will result in atmospheres that will be riddled with "resistance to change" personalities. I believe that organizations develop a cultural behavior by the influences of their management and by their mission goals, which over time become embedded in the attitudes of the personnel. These embedded attitudes are important because they are the cultural differences that leadership will need to change to make DHS a more efficient organization.

The strategic leaders of DHS will encounter these resistances on a daily basis and in the foreseeable future. One of the hardest challenges will be implementation of changes impacting the cultural environment. In a recent study on homeland security, the Government Accounting Office (GAO) found that no level of government thought that the information sharing process for homeland security was effective.[2] This report found that information on threats, methods, and techniques of terrorists is not routinely shared with the various levels of homeland security because of cultural resistance to providing information to other agencies.[3]

Although it is necessary to have different systems serving many different functions, DHS will find highly effective functional advantages to combining many of their systems through integration. For example, integrating their many systems into a centralized database that lists names of all terrorist suspects would be beneficial at the federal, state, and local level. Of course, whenever integration takes place, there is always a consolidation of functions and systems affecting several areas. The leadership of DHS will need to determine what levels of systems require integration and if it is cost effective.

In conjunction with system integration, the DHS will need to develop a process to systematically, and actively, manage the knowledge base within their consolidated organizations. Managing this knowledge must include the domains of structured internal knowledge, external knowledge, and informal internal knowledge.[4] If designed properly, DHS can gather any internal knowledge from their personnel and databases, at the same time relevant external information is being processed from their outside sources. Informal internal knowledge is often called tacit knowledge, is usually poorly documented, and resides in the expertise and experience of individual employees.[5]

Developing decision-making systems will remain a challenging aspect for the DHS. Information technology will help strategic leaders communicate management decisions. A major remaining challenge will be the method used to prioritize decisions based upon captured information. Managing this knowledge will be critical to the mission of DHS and could reap

benefits very advantageous in the war on terrorism. For example, using a risk-based scoring system by which DHS can assess the threat or risk posed by a suspected terrorist or individual getting on a specific flight could be beneficial to the Global War on Terrorism. [6]

CULTURAL CHANGE

Prior to the events of September 11, 2001, the U.S. Army War College Strategic Studies Institute sponsored a major conference that examined what the Department of Defense must do to insure domestic tranquility, and provide for the common defense, given the increasing threats to the U.S. homeland.[7] The main theme that was scattered throughout the strategic level presentations was the many cultural challenges facing the various levels of government. Combining the 22 agencies has brought together different institutional and personal values as well as different priorities of management styles to create an environment of cultural differences within the DHS organization. Cultural differences can profoundly affect organizational standard operating procedures and is prevalent within the various levels of the Department of Homeland Security. The strategic leaders of DHS are facing a host of specific barriers from protecting local information to differences in technical approaches and do not necessarily have the expertise or time to turn the tide with cultural change. It may take an entire organizational generation change to put the entire DHS on the right track. There will be daily occurrences of cultural differences at DHS, which the management will have to grapple with amongst the various consolidated organizations. For example, at a recent Homeland Security Conference there was much discussion about the need to adopt a culture of “Need to Share (Information)” as opposed to a culture of “Need to Know (Intelligence)”.[8] And during an interview, Major General Dale Meyerrose, Director of Architectures and Integration at Northern Command, stated that the pentagon faces many cultural barriers as it works with other federal agencies within DHS.[9]

Until another generation of workers infiltrates the cultural biases of DHS, the cultural difference within the various DHS organizations will continue to produce different leadership agendas. In most cases, I believe older, more senior, leaders will resist new ideas and changes and become barriers themselves hampering the progress of any changes. Strategic leaders at DHS must realize that their territories have cultural barriers and that they must assist in modifying these barriers within their respective areas of responsibility as soon as they can. In reference to information technology, the cultural differences can also affect the way organizations intend to use the capabilities of their information technology or not use it. For example, Japanese organizations use fax capabilities extensively and have been reluctant to

take advantage of e-mail capabilities, believing that e-mail is poorly suited for intra-group communication.[10] I would venture to say that within the Department of Homeland Security, there are hundreds of processes that use a microcomputer to produce a product, which is then faxed to another area that takes the facsimile and re-types the same information into another microcomputer. There are many of these kinds of cultural barrier surrounding the processes within any organization and they are not easily overcome. For example, officials at the National Emergency Management Association, which represents state and local emergency management personnel, stated that they continue to have problems receiving critical intelligence information from DHS and that this has hampered their ability to help pre-empt terrorists before they strike.[11]

In order to adopt the kinds of strategic systems useful to DHS, changes will be required in mission goals, relationships with stakeholders, internal operations, and the information architecture. These changes will have an affect on the social and technical elements within the various organizations and are referred to, in most technical circles, as strategic transitions.[12] Basically, it is the changes and movement between levels of the socio-technical systems within an organization. In a socio-technical perspective, the performance of a system is optimized when both the technology and the organization mutually adjust to one another until a satisfactory fit is obtained.[13] How much socio-technical change occurs depends on the specific circumstances. There is a clear relationship between the DHS and the internal structure of the combined organizations. As DHS moves to make information systems part of the overall strategy, the internal structure must also change to reflect the new developments. There will be a requirement to redesign various organizational processes to make effective use of the information technology systems.

In order for DHS to be successful in meeting their mission requirements, the barriers that block the sharing of data across functions must be overcome at all levels. The personnel within the various departments, divisions, sections, and work areas must work together closely to share information among operations, services, and security functions. The Government Accounting Office (GAO) reported in August 2003 that overall “no level of government perceived the information sharing process as effective, particularly when sharing information with federal agencies”.[14] Information on threats, methods, and techniques of terrorists is not routinely shared and the information that is shared is not perceived as timely, accurate, or relevant.[15] The GAO report also revealed that federal officials have not yet established comprehensive processes and procedures to promote sharing. Federal representatives said that state and city officials had no way to secure and protect classified information, lacked federal security

clearances, and integrated databases, all of which hampered their ability to share information. With the increased importance on homeland security, how can this continue to happen? Personally, I believe there is a cultural resistance within DHS that directly resists process changes required. In order to provide for an effectively managed DHS, leaders need to maintain open minds and review processes related to information sharing at all levels. After review, there will be many recommended improvements that will require redesigning work processes numerous times to continually improve the overall communications and sharing of data at all levels (federal, state, city, county). Other organizational changes may be required as well. For example, the standard operating procedures within DHS may need to be redesigned so that data is shared internally amongst the appropriate functional areas.

Subject matter experts are critical to changing any of the DHS processes. Subject matter experts are those employees that are resident experts within their functional areas. First, however, you must have wide acceptance by these experts. The majority of the DHS employees have vested interests in improving the homeland security capability of the United States. They have to be convinced to look at their own processes and be willing to experiment to improve them. Their vested interests revolves around having a safe and secure environment in which to work, live, and raise their families. It is human nature to resist change, but once convinced there is a better way people quickly add their inputs to the overall improvement process.[16]

SYSTEMS INTEGRATION

Hardware, software, and telecommunications pose special technical challenges within DHS. The major hardware challenge will be finding some way to standardize the organizations computer hardware platform when there is so much variation from operating unit to operating unit and from state and local areas. The leaders need to think carefully about where to locate the organization's computer centers and how to select hardware suppliers. The major software challenge is finding applications that are user friendly and enhance the productivity of the work teams.[17] A major telecommunications challenge is making data flow seamlessly across networks shaped by disparate mission statements.[18] Overcoming these challenges requires that the DHS ensure their systems integration and connectivity plan is developed for a national level capability. According to a recent GAO report, the Federal Bureau of Investigation (FBI) still lacks an IT strategy for modernizing its IT systems because the agency has not made such a strategy a priority. In their report, GAO states that research has shown that to modernize an IT

environment, it requires development of a well-defined and enforceable enterprise architecture plan.

The development of national information system infrastructures based on the concept of core mission systems raises questions about how the newer core systems will fit in with the existing suite of applications developed throughout the various areas of DHS. The goal will be to develop national, distributed, and integrated systems.[19] The correct solution often will depend on the DHS history of the organization's systems and the extent of commitment to legacy systems. For example, finance and budget systems have relied on IBM proprietary equipment and architectures. It is difficult and costly to abandon that equipment and software. Newer DHS functional areas may find it easier to adopt UNIX-based systems which are more cost effective in the long run, provide more power at a cheaper price, and have options for future expansion.[20]

After the leaders chose a hardware platform, the question of standards must be considered. There are many functional areas that have the same hardware and software, but it does not guarantee that their systems are integrated and have common functions.[21] The DHS strategic leaders for IT must establish data standards, as well as other technical standards, for areas to comply. This standard is required for data entry purposes. If data is entered into a database, it has to be retrievable. For example, there are many methods to enter dates into the database. In several functional areas, it is entered as month, date, year (030104). While in other areas, it might be entered as year, month, day (040301). Performing a sort function would reveal different results. Another example is identification of equipment. A data entry for a computer could be CPU, micro, computer, or microcomputer.

Compatible hardware and communications provide a platform but do not necessarily give the functional capabilities required for the organization.[22] For example, the organization could put a budgeting module in place that gives everyone within the comptroller function the required information but does not provide the information to the functional manager or the executive offices. The strategic leaders of DHS must ensure that their infrastructure is designed so the entire enterprise has access to required information. Critical to this process is choosing appropriate software that has the capability of developing a national core infrastructure. The development of core systems with effective software poses unique challenges for the DHS. How will the older systems interface with the new systems? Entirely new software interfaces must be built and tested if the older systems are to be kept in place at local areas. These interfaces can be costly and messy to build. If new software must be created, another challenge is to build it so that it can be used by multiple DHS areas from different locations at

the national level. In addition to integrating the new with the old systems, there are also problems with human interface design and functionality of the systems. For example, to be truly useful for enhancing the processes of DHS, software interfaces must be easily understood and mastered. Graphical user interfaces are ideal assuming that English will be the standard language.[23]

The majority of managers within organizations are trained to manage specific functions related to their mission statement or tasking.[24] My opinion and past experience has shown that managers and planners for information technology operations are rarely trained or involved with the concept of optimizing the performance of their organizational enterprise. Taking the DHS into an enterprise system concept of operation of their information technology will require that DHS strategic leadership direct their managers to take a much larger view of their roles within the entire organization. To be successful in developing a plan for integration of all DHS systems, the organizations must work together for a common goal. The investment to migrate any organization into an enterprise system is costly and normally takes a long period of time to accomplish.[25] The leaders of DHS need to take this into account as they make management decisions and also include their functional managers in the design of the shared, enterprise vision.

In the majority of organizations the typical design, within the functional areas, has separate systems supporting single application processes.[26] This is the case within DHS and requires that a review be made to consolidate processes that are duplicated within the various different organizations. For example, there is duplication of systems and efforts within the financial and logistics support areas of the agencies consolidated under DHS.

A specific area that must receive special emphasis from the DHS strategic leadership is the overall security of the IT infrastructure. The DHS Secretary Tom Ridge recently announced that DHS is providing an information network that will be expanded to link every state and major urban area to federal officials by fall of 2004.[27] This national information network will be expanded to provide classified information up to the “secret level” by using the current DoD classified network.[28] DHS should use the more economical virtual private network (VPN) capabilities to provide security for their network expansion. Instead of using private or leased lines like traditional DoD networks, virtual private networks (VPNs) use the commercial Internet infrastructure to communicate with distant computers.[29] VPN technology provides security without high costs. By using VPN technology, DHS could possibly reduce networking costs by 50% or more. VPN technology does not require establishment of a firewall infrastructure, which drastically reduces overall network costs. Another advantage of VPN technology is the ease

with which they can be set up and accessed. It could take months to install a leased line in certain parts of the country. Also, mobile users can tap into VPN infrastructure using dial-up connectivity.

It is my opinion that technological advances will continue to fall in price and gain in power providing for a more robust national network for DHS. Networks capable of communicating and computing anytime, anywhere based on satellite systems, digital cellular phones, and personal communication services will make it easier to coordinate work and information in many parts of the globe that cannot be reached by existing ground supported systems.[30] For example, a border crossing official in Texas, could send an identification request to their home base in Washington effortlessly and expect an instantaneous reply.

KNOWLEDGE MANAGEMENT

When the president established the Office of Homeland Security in 2001, he designated a single focal point to coordinate efforts for securing the United States from terrorist attacks.[31] The office was charged with responsibilities that included coordinating threat and intelligence information. When the Strategy for Homeland Security was issued it was "national" in scope to include federal agencies, states, localities, and private-sector entities.[32] Currently, the United States does not have a system for identifying who has overstayed their visa, nor an effective ability to identify and locate visitors who may pose a security threat. Recently, the INS implemented a system, which uses biometric information to identify travelers entering and exiting the country. [33] Information captured with this biometric identification system needs to be shared amongst appropriate levels of the homeland security program. This system is an example of the many information technology capabilities that are available today which can be interfaced with other systems that contain vital information for homeland security. Another system that could be interconnected would be the Department of Justice Regional Information Security System (RISS) as well as other law enforcement programs. These various systems could be used to transmit photos, maps, and vast amounts of data from open sources to include articles from foreign newspapers.

Putting this type of information into databases that can be maintained, as well as searched, will provide a knowledge capability that can be managed at the appropriate levels within the Department of Homeland Security. Another aspect that the strategic leaders of DHS must consider is the sharing of their systems with authorized private sector entities. For example, businesses that provide technical equipment and/or services that could be used by terrorist cells need access to this information. Giving them access to the data would provide a

method to check terrorist activities or suspects prior to selling high-risk items. There are several businesses in Florida that provided private pilot lessons that could have verified personal information or confirmed that individuals are authorized to receive this type of educational service. The senior leadership at DHS should ensure that federal systems are available to be utilized by the private sector and even foreign countries for verification. Providing this capability could prevent future terrorist events from happening.

Although information technology within the United States is the most advanced in the world, our country's systems cannot support the management of knowledge for the missions assigned to the Department of Homeland Security. [34] Much of the needed information exists in disparate databases scattered among federal, state, and local entities. In many cases, the information cannot be shared across the same level of government or between federal, state, and local governments. The databases used for law enforcement, immigration, intelligence, and public health surveillance have not been connected in ways that allow us to recognize informational gaps.[35] As a result, government agencies have not been able to share terrorist information such as the terrorist watch lists with other agencies. This causes mistakes that continue to occur with visa applications and border controls checking against the watch lists. The strategic leaders of DHS must make this management of knowledge capability a critical mission requirement.

The collection of information on terrorist activities within the United States is important and could be enhanced by providing the local law enforcement agencies with a capability to input their information into a central database. Local law enforcement efforts include documenting any encounter with individuals. Providing a method for local law enforcement agencies to input their data would enhance the overall information gathering capabilities of DHS.

A strategic asset of DHS is the knowledge that they obtain from all sources and the centralization of this information into an easily accessible database. Managing this asset is a complex operation and will require that DHS manipulate information, review social relations, scan personal knowledge, and track specific individual skills simultaneously and in real time. Managing knowledge must be an attribute of DHS that can then be exported to sister agencies.

Maintaining a knowledge based DHS has important consequences for how the organization is managed and how their information technology is utilized. The strategic leaders of DHS should be focused on gathering, acquiring, storing, and dissemination of information and knowledge. At the same time, DHS must emphasize the importance of building new knowledge <u>into</u> the organization. Maintaining teams of subject matter experts becomes important in this process because problem solving often requires the input of many people who work in the

functional areas. DHS strategic leaders should include in their long-range strategies, procedures which focus on strengthening its core knowledge competencies and building the DHS knowledge base.

DECISION-MAKING

Decision-making will be one of the more challenging roles for the DHS. Information technology has helped leaders communicate and distribute information, but it has provided only limited assistance for management of decision-making.[36] Within each of the levels of decision-making, decisions can be either programmed or non-programmed. Rational models of decision-making assume that individuals can accurately choose alternatives and consequences are based on the priority of their mission requirements and goals.[37] Behavioral research has revealed that individuals appear to muddle through decisions in a logical order or they select alternatives by their specific style and frame of reference. If information systems are configured properly, they can support individual and organizational decision-making. Information systems have been helpful in performing informational and decisional roles.[38] These same systems can be made to be less formal and could be useful in the decision-making process within DHS. The design of the systems must be able to accommodate high flexibility as well as tailored to the environment. Middle managers and senior managers at DHS can use management information systems (MIS) and executive support systems (ESS) to monitor day-to-day operations at any level of detail needed. Decision-support systems (DSS) and ESS do not necessarily guarantee more accurate and predictive forecasting. This form of decision-making relies on many factors such as the skill of the manager.[39]

The DHS strategic leaders can also use decision-making information systems to give managers and employees more responsibility and decision-making power. Electronic mail, and other network-based forms of communication can enable DHS leaders to broaden their span of control and manage lower level organizations. Group communication VTC provides a capability to establish and manage flexible work groups and short-term task forces around the United States thus quickly bringing the right mix of skills to bear regardless of mission requirement.[40] Information as well as direction can be rapidly distributed to employees at local levels who can act independently.

TELECOMMUNICATIONS

As stated by Governor Ridge on November 27, 2001 at the Homeland Security and Defense Conference, one of the things that will make the missions of Homeland Security easier will be the infusion of technology. A significant investment this country will have to make is

equipping some of the DHS agencies with more advance telecommunications. Linking together the systems and people of DHS into a single integrated network just like the phone system but capable of voice, data, and image transmissions. However, integrated nationwide area networks are difficult to create. For example, many areas of the country cannot fulfill basic telecommunication needs such as obtaining reliable circuits, coordinating among different carriers and regional telecommunications authority, and obtaining standard agreements for the level of telecommunications service provided.[41] Other problems associated with maintaining connectivity of a wide area network are costs, network management, installation delays, poor quality of service, changing user requirements, disparate standards and total network capacity.[42]

Harnessing the telecommunications capabilities of DHS into a single high-speed digital telecommunication network will be an expensive but necessary venture for DHS. Communication amongst the many DHS geographically dispersed sites will require an effective real-time infrastructure. DHS must have their telecommunications interlinked to perform the many functions required and must maintain a secure environment protecting it from the commercial Internet. The insecurity of the commercial Internet will require that DHS include protective equipment (firewalls, intrusion detection systems) within their infrastructure design to protect their resources.

CONCLUSION

It is obvious that the strategic leaders of Department of Homeland Security will face daunting tasks in the future years. If the nation intends to win the war on terrorism, DHS will have to continue to make changes and overcome cultural differences within the organization to maintain a tactical edge and accommodate future antiterrorist initiatives. It is evident that technological advances are going to significantly change the capabilities of DHS. To increase the effectiveness and maintain credibility within DHS, decisive action is required on the part of the strategic leadership DHS must continue to upgrade the national detection and deterrence capabilities so that the confidence of our leaders and citizens can remain strong.

DHS must find ways to develop systems, which will manage gathered information and knowledge while supporting all aspects of homeland security. This will be a painstaking process taking several approaches and will have to be continually monitored for modifications. Decision-making has to be automated so it encompasses each specific implication that could be encountered by DHS.

The strategic leaders of DHS are encountering an enormous challenge in reorganizing and integrating 22 disparate agencies with nearly 180,000 employees into four mission organizations. It is my argument that by having positive control of the five (5) challenging areas of cultural change, systems integration, knowledge management, decision-making, and telecommunications, DHS can successfully maintain an efficient and effective organization that will provide a protective wall between terrorist activities and the homeland of the United States. Due to my past experience, I believe it is best that DHS use the expertise of outside consultants to develop a plan to overcome any cultural barriers and to integrate their systems. I believe that DHS has the expertise internally to solve any problems with knowledge management and their decision-making. I would recommend the DHS use the existing DoD telecommunications infrastructure to deploy their national information network.

This overall challenge presents an opportunity for DHS to become the model of management excellence for IT resources while effectively winning the battle against terrorism.

> To succeed in their mission, leaders of the new department must change the culture of many agencies, directing all of them toward the principal objective of protecting the American people
>
> —President George W. Bush

WORD COUNT=4868

ENDNOTES

[1] National Strategy for Homeland Security, Department of Homeland Security, July 2002, U.S. Government, 1.

[2] Government Accounting Office Report-03-760, *Homeland Security: Efforts to Improve Information Sharing Needs to be Strengthened,* August 27, 2003, U.S. Government, 2.

[3] Ibid., 3.

[4] G. David Garson, *Information Technology and Computer Applications in Public Administration: Issues and Trends,* Idea Group Publishing, 1999, 101.

[5] Ibid., 107.

[6] Chloe Albanesius, *Technical Coordinators for Homeland Security Face Challenges*, National Journal's Technology Daily, September 23, 2003, 1.

[7] Dr. John J. Hamre, *Papers from the Conference on Homeland Protection,* October 2000, 17.

[8] E-Government Homeland Security Conference Minutes, 2-3 Dec 2003, Washington, D.C., 1.

[9] Government Executive Magazine, *Cultural Barriers a Challenge for Pentagon in Homeland Mission,* November 25, 2002, 1.

[10] Kenneth and Jane Laudon, *Management Information Systems,* Prentice Hall, 2000, 534.

[11] Government Accounting Office Report 02-490T, *Homeland Security: Progress Made; More Direction and Partnership Sought,* March 12, 2002, U.S. Government, 10.

[12] Kenneth and Jane Laudon, *Management Information Systems,* Prentice Hall, 2000, 61.

[13] Ibid., 13.

[14] Government Accounting Office Report-03-760, *Homeland Security: Efforts to Improve Information Sharing Needs to be Strengthened, 27 August 2003*, U.S. Government*, 2.*

[15] Ibid., 3.

[16] G. David Garson, *Information Technology and Computer Applications in Public Administration: Issues and Trends,* Idea Group Publishing, 1999, 24.

[17] Kenneth and Jane Laudon, *Management Information Systems,* Prentice Hall, 2000, 384.

[18] Ibid., 385.

[19] Ibid., 173.

[20] Andrews S. Targowski, *Global Information Infrastructure,* Idea Group Publishing, 1998, 97.

[21] Ibid., 22.

[22] Ibid., 54.

[23] Kenneth and Jane Laudon, *Management Information Systems,* Prentice Hall, 2000, 199.

[24] Ibid., 284.

[25] Ibid., 577.

[26] Shailendia Palvia, *Global Issues of Information Technology Management,* Idea Group Publishing, 1992, 8.

[27] Greta Wodele, *Ridge Unveils Plans for National Information Network* , National Journal's Technology Daily, 24 February 2004, 1.

[28] Ibid., 2.

[29] Kenneth and Jane Laudon, *Management Information Systems,* Prentice Hall, 2000, 301.

[30] Ibid., 264.

[31] Office of Management and Budget*, Fiscal Year 2004 Budget Submission* , U.S. Government, 23.

[32] George W. Bush, *Homeland Security Act of 2002 (HR. 5005),* U.S. Government.

[33] Government Accounting Office Report-03-760, *Homeland Security: Efforts to Improve Information Sharing Needs to be Strengthened,* August 27, 2003, U.S. Government, *2.*

[34] Government Accounting Office Report 02-490T, *Homeland Security: Progress Made; More Direction and Partnership Sought,* March 12, 2002, U.S. Government, 10.

[35] Government Accounting Office Report-03-760, *Homeland Security: Efforts to Improve Information Sharing Needs to be Strengthened,* August 27, 2003, U.S. Government, 3.

[36] Kenneth and Jane Laudon, *Management Information Systems,* Prentice Hall, 2000, 109.

[37] Ibid., 111.

[38] Ibid., 39.

[39] Ibid., 111.

[40] Shailendia Palvia, *Global Issues of Information Technology Management,* Idea Group Publishing, 1992, 74.

[41] Ibid., 74.

[42] Ibid., 75.

BIBLIOGRAPHY

Albanesius, Chloe, *Technical Coordinators for Homeland Security Face Challenges*, National Journal's Technology Daily, 2003.

Bush, George W., *Homeland Security Act of 2002 (HR. 5005)* U.S. Government, Washington, D.C., 2002.

Garson, David G., *Information Technology and Computer Applications in Public Administration,* Idea Group Publishing, Hershey, Pennsylvania,1999.

Hamre, John J., *Papers from the Conference on Homeland Protection*, U.S. Government, Carlisle, Pennsylvania, 2000.

Laudon, Kenneth and Jane, *Management Information Systems*, Prentice Hall, Upper Saddle River, New Jersey, 2000.

Palvia, Shailendia, *Global Issues of Information Technology Management*, Idea Group Publishing, Hershey, Pennsylvania, 1992.

Strohm, Chris, *Cultural Barriers a Challenge for Pentagon in Homeland Mission*, Government Executive Magazine, November 2003.

Targowski, Andrew S., *Global Information Infrastructure*, Idea Group Publishing, Hershey, Pennsylvania, 1998.

U.S. General Accounting Office. *Homeland Security: Progress Made; More Direction and Partnership Sought, GSO-02-490T*, Washington, D.C., 2002.

U.S. General Accounting Office. *Homeland Security: Efforts to Improve Information Sharing Needs to be Strengthened, GAO-03-760*, Washington, D.C., 2003.

U.S. Office of Management and Budget, *Fiscal Year 2004 Budget Submission*, Washington, D.C., 2002.

Wodele, Greta, *Ridge Unveils Plans for National Information Network* , National Journal's Technology Daily, 2004.